iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** IV **Month of publication:** April 2017

DOI: http://doi.org/10.22214/ijraset.2017.4116

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Secure Searching Encrypted Data over Cloud

Nikita Bharat Nerkar[1], Samrudhi Haribhau Khairnar[2], Rituja Nandkishor Pawar[3], Prof. Amit. G. Patil[4]
[1,2,3,4]*Sandip Foundation*

Abstract: ***Cloud is one of the type of application which can be used by using Internet for storing, inserting or managing the data for very less cost. Due to the increasing popularity of the cloud computing more and more data owners are motivated. Their data to cloud Server for great convenience and reduced cost in data management. Sensitive data should be encrypted before outsourcing for privacy requirements. A "Greedy Depth-First search" algorithm is provide efficient multi-keywords ranked search and it used for achieving efficient searching in the large database. It provide tagged base Security to multimedia files like Audio, Video files by using AES algorithm. and it's also utilized encryption and decryption purpose KNN algorithm used for protecting data on the cloud from different attacks.***
Keywords: ***Searchable encryption, multi-keyword ranked search, dynamic update, cloud computing.***

I. INTRODUCTION

Cloud is a term which is frequently used to store large data. The another type is to stored data in cloud computing used for sharing the devices and Data to the computers or other devices or LAN (Local Area Network).cloud computing is model in IT Infrastructure. Cloud computing providing services to the end user, business and Industry. If Data is important then private cloud is used. In other type of Cloud such as public cloud providers included Amazon service, Google, Microsoft, other shopping website's. The last type of Cloud is hybrid cloud is the combination of private cloud and public cloud. cloud computing uses three categories like infrastructure as a service, platform as a service, and last is software as a service. In simple words cloud computing is the process of delivering of computing services to the server ,storage, databases, networking, software, analytics and more over the Internet. Company's offering these computing services are called cloud providers and typically charge for cloud computing services based on usage , similar to how you are billed for water or electricity at home.

The main use of cloud computing provide online service to send email, edit documents, watch movies ,educational purpose. The very first cloud computing services are decade old ,but already a variety of organizations .following things can done by cloud first is creating new application and provide services, second is steam audio and video, third is delivering software on user demand, fourth is analyzed data for pattern's and make predictions.

There are various advantage of beneficial to the Cloud services for uploading important information such as personal email, financial data ,government documents etc. The data which is stored on to the Cloud is not mean all data is stored securely it requires some security keys .so one method to provide Secure Data on cloud is in encryption format. When authorized person want to access data that can be Encrypted by using security key.

In this paper we describe encryption description process. This process in including four following entities like data owner ,data users, cloud server, kdc that is key distribution center. The confidential data can be accessible only for the data users which are authorized users and authentication is sharing the secret key to the user.to provide encryption by using AES algorithm. We are providing key distribution center is part of a cryptosystem intended to reduce the risks to interchangeable keys. KDC often operate in systems within which some users may have permission to use certain services at some time and not at others. The main operation of KDC is a typical operation with a KDC involves a request from a user to use some services. The KDC will use cryptographic techniques to authenticate requesting users as themselves. It will also check weather an individual user has the right to access the service requested .if the authenticated user meets all prescription condition the KDC can issue a ticket permitting access .KDC can identify the user identity and provide token. By using token it is easy to find particular documents.so it required less time .the AES algorithm used symmetric keys to encryption and decryption process.it encrypt and decrypt the document files, text files, multimedia files.it does not require two keys for encryption and decryption process. The plain text given is divided into 128 bit blocks as consisting of 4*4 matrix of bytes .the first four bytes of a 128 bit input block occupy the first column in the 4*4 matrix.

The tree - based index structure is proposed and to achieve highest search efficiency Greedy Depth first search algorithm is utilized the b- tree algorithm is used for index generation. Index can stored Data level wise .high priority data can stored on high level .The highest priority can be identify by using frequency count .frequency count is defined how many time particular statement or file requested or executing.

©IJRASET: All Rights are Reserved

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

II. PROPOSED SYSTEM

This paper represents a system architecture which is combination of data user, cloud server and data owner .The data owner encrypts the data before uploading them to the cloud server. To perform a search, the data user must be authorized by the data owner. The user generates a trapdoor function when the search request is sent to the cloud server. The server computes the ranked score based on the index and trapdoor. Data used can perform multi-keyword ranked search and dynamic updating like insertion and deletion on data. In this system architecture there are three main block Data owner, Data User, Semi trusted cloud server.

A. Data Owner

Data owner is the owner of the data which wants to outsource their sensitive information like emails, personal health records, financial data, government documents, etc. to the cloud .As the data owner is outsourcing there sensitive information there is necessity privacy and security to data.

Data Owner has the collection of documents that can be in text format or multimedia f files. First the data owner uploads the data or multimedia files on cloud. The data owner has collection of documents like F={f1,f2,f3,f4,……fn}.Then data owner has does the index generation. Index generation means data owner firstly builds the index I from document collection F and then it generates encrypted document collection. After generating the encrypted document data owner outsource the data to the cloud server and securely distribute secret key to the authorized data user.

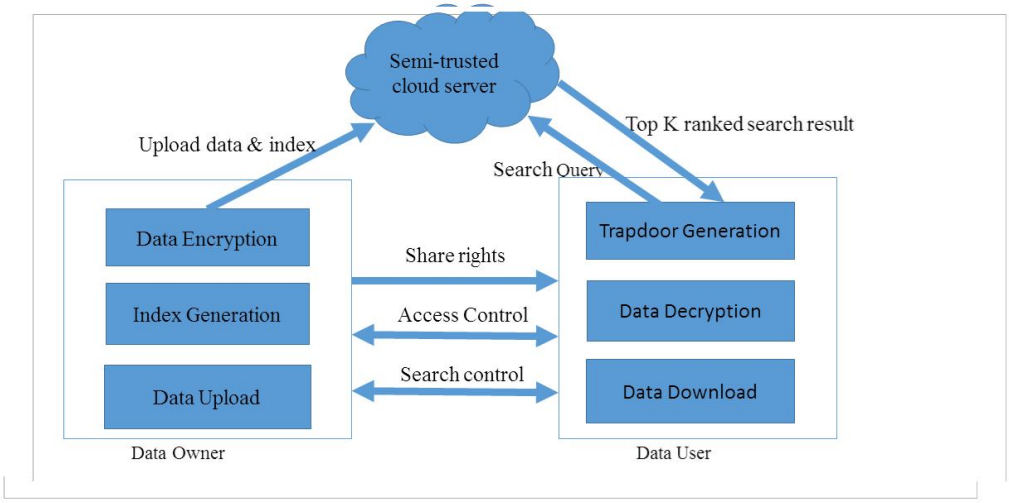


Fig. Encryption and Decryption Process

B. Data User

Data user is the authorized user to access the document of the data owner. Firstly data user downloads the data that he wants to access. Then data user can generate a trapdoor function to fetch the encrypted document from cloud server. Then data user can decrypt the data by using secret which is shared by the data owner the authorized user i.e. private key or public key. For sharing the secret key AES algorithm is used. In AES algorithm concept of symmetric key is used Semi trusted Cloud server.

C. Cloud Server

Cloud server stores the encrypted documents collection and encrypted searchable tree index I from data owner. Cloud server executes trapdoor function which is received from data user and finally it returns back corresponding collection of top k ranked search results for Encrypt document.

D. KDC

KDC is another important entity of the proposed system. KDC is the “Key Distribution Center” of the system. Firstly the data owner do the registration on KDC with several fields before registration on the cloud. After doing the registration on KDC it generates

©IJRASET: All Rights are Reserved

token for the user identification. KDC provides the secret keys to the valid user or authorized user. KDC generates the token for authorized user verification.

III. ALGORITHM

Step 1:- Derive the set of round keys from the cipher key.
Step 2:- Initialize the state array with the block data (plaintext).
Step 3:-Add the initial round key to the starting state array.
Step4:-Perform nine rounds of state manipulation.
Step 5:-Perform the tenth and final round of state manipulation.
Step 6:-Copy the final state array out as the encrypted data (ciphertext).

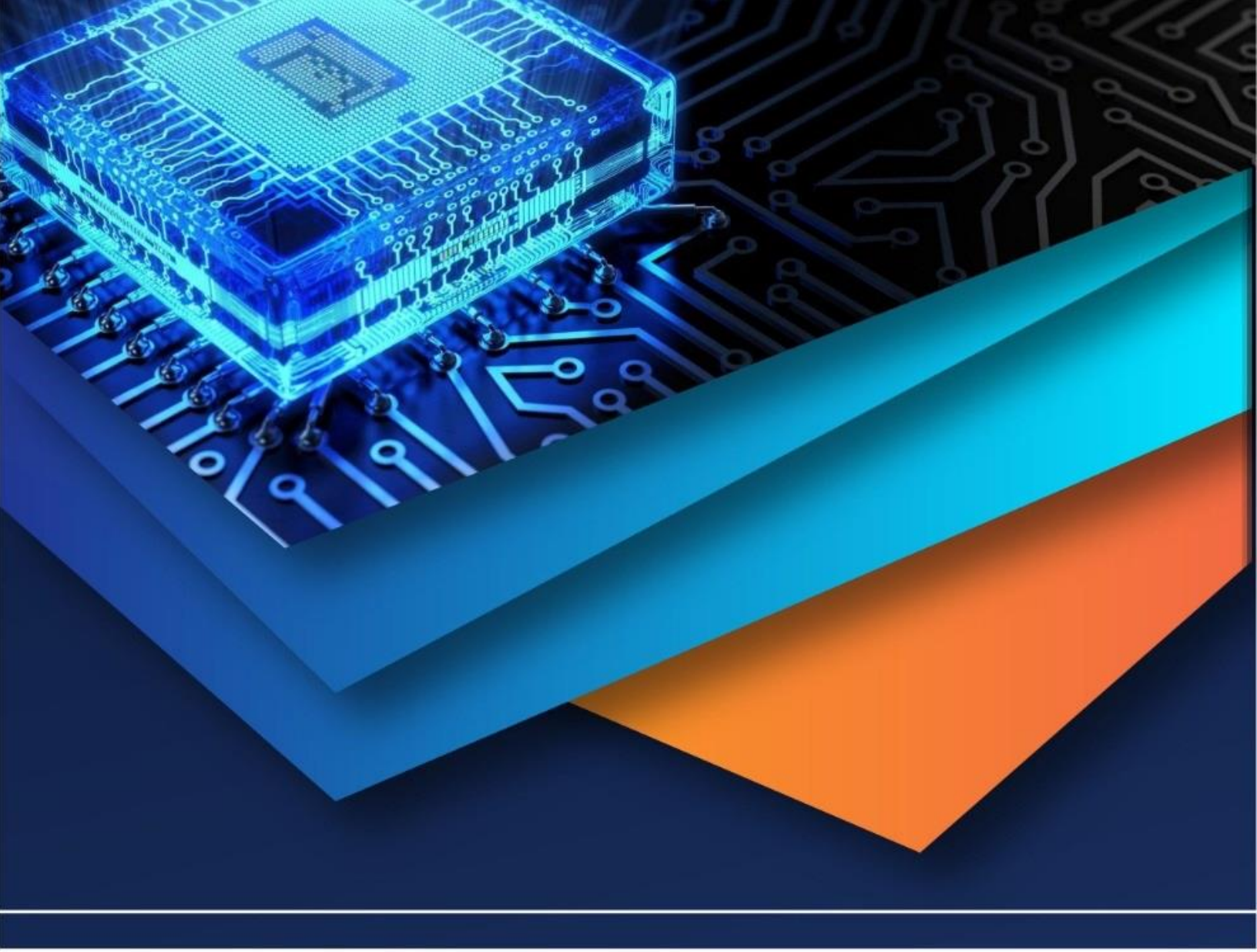
IV. CONCLUSION

This paper proposes secure efficient dynamic search scheme. I which it supports multi-keyword ranked search but also dynamic insertion and deletion of data and multimedia files using symmetric key .This system also propose greedy depth first search algorithm for achieving better efficiency and B-tree algorithm for index generation is implemented for protecting system from different attacks still there are various problem which can develop in future. We will try to improve searchable encryption scheme to handle these challenge problems.

REFERENCES

[1] Zhnghua Sheng:Zhigiang ma:Lin Gu :Ang Li," A Privacy Protecting File System on public cloud Storage Cloud and Services Computing",2011
[2] Ibrahim,A;Hai Jin,Yassin ,A;Dewingzocs, "Secure Rank -Ordered Search Of Multi-keyword search of multi-keyword trapdoor over encrypted cloud data",2012.
[3] chengyu Hu; pengtao Liu ,"Public key Encryption with Ranked Multi-keyword Search" ,2013
[4] Zhihua Xia, Member, IEEE, Xinhui Wang, Xingming Sun, Senior Member, IEEE,and Qian Wang, Member, IEEE," A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL: PP NO: 99 YEAR 2015

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)